

## UNITED STATES DISTRICT COURT

for the  
Western District of Texas**FILED**

FEB 06 2015

CLERK, U.S. DISTRICT COURT  
WESTERN DISTRICT OF TEXAS  
BY [Signature]

DEPUTY

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)6105 Spahn Street, Midland  
Texas 79706Case No. MO:15-MJ-064

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

6105 Spahn Street, Midland, Texas 79706 (More fully described in Attachment "A")

located in the Western District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 USC 2252 (a)(4)

Possession of Child Pornography

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[Signature]  
Applicant's signature

Kris Knight

Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 2-6-15[Signature]  
Judge's signatureCity and state: Midland, Texas

Robert A. Junell

United States District Judge

Printed name and title

## ATTACHMENT A

### DESCRIPTION OF PREMISES TO BE SEARCHED

The residence, located at 6105 Spahn Street, Midland, Texas 79706, is a single story home with brown, tan, and grey brick siding. The home has tan stone and wood trim. The numbers "6105" are affixed to the home on a plaque.

A white SUV bearing Texas license plate 292 5AY was parked in the driveway of the residence. Records checks show that that license plate Texas 292 5AY was cancelled in 2012.

The search may include: one white SUV bearing Texas license plate 292 5AY.

## ATTACHMENT B

### ITEMS TO BE SEIZED

Items to be seized include any and all evidence, fruits and instrumentalities pertaining to violations of Title 18 United States Code, Section 2252 and which may be more particularly described as follows:

Any instructions, programs or recording stored in the form of electronic or magnetic media which are capable of being intercepted by a computer or related components. The items to be seized include operating systems, application software, utility programs, compilers, interpreters, and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio or other means of transmission.

Electronic devices, computer hardware, software, passwords, data security devices, and computer-related documentation. Electronic devices and computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices, (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct

All cellular phones, laptops, netbooks, e-books, tablets, and any other electronic media storage devices.

This is property that constitutes evidence of the commission of a criminal offense and property designed and intended for use and which is and has been used as the means of committing a criminal offense in violation of Title 18 United States Code, Section 2252.

## **AFFIDAVIT**

I, Kris Knight, being duly sworn do hereby depose and state as follows:

I am a Special Agent of the Department of Homeland Security (DHS). I have served as a federal law enforcement agent for the last seven years. I am currently assigned to the Homeland Security Investigations (HSI) office in Midland, Texas where I am responsible for conducting investigations into violations of Federal law including laws involving the possession, manufacturing, and distribution of child pornography.

As an HSI Special Agent my duties include the enforcement of federal criminal statutes involving child exploitation laws, to include; receiving, manufacturing, collecting, and distributing child pornography. I received training at the Immigration and Customs Enforcement Special Agent Training (ICE-SAT) Academy at the Federal Law Enforcement Training Center (FLETC), to investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252. I have worked closely with other federal law enforcement agents who have engaged in numerous investigations involving child pornography and who have received training in the area of child pornography and child exploitation.

The statements contained in this affidavit are based on an investigation conducted by HSI Special Agents. This affidavit is submitted in support of an application for an search warrant authorizing the search of 6105 Spahn Street, Midland, Texas 79706, (more fully described in Attachment "A") and the seizure of evidence (more fully described in Attachment "B") which is incorporated herein by this reference, all located within the Western District of Texas, Midland Division. This affidavit contains information known to your affiant personally and to other law enforcement officials involved in the investigation.

Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252 are located at 6105 Spahn Street, Midland, Texas 79706 (hereafter referred to as "Subject Premises"), and within computers, electronic devices, related peripherals and computer media found at the "SUBJECT PREMISES". Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

### **APPLICABLE LAWS**

Title 18 United States Code 2252

## **BACKGROUND REGARDING THE INVESTIGATION**

HSI Special Agents discovered that a Peer to Peer (P2P) network user, utilizing Internet Protocol (IP) addresses 72.48.82.156, made three containing known images/videos of child pornography available for download through the Peer to Peer (P2P) Ares network between May 23, 2014, and June 2, 2014. The Internet Protocol (IP) addresses used to facilitate this act, resolved to an account with Grande Communications subscribed to by Al Weinkauff, 516 N. Loop 250 West, Apt. 1601, Midland, Texas 79703.

This case was assigned to the HSI Midland, Texas case for local investigation and possible prosecution.

## **SUMMARY OF THE INVESTIGATION TO DATE**

HSI Special Agents conducted an investigation into the trading of files containing known child exploitation using the Peer to Peer (P2P) file sharing Ares network. Homeland Security Investigations (HSI), Special Agent (SA) Kris Knight, utilized law enforcement databases to locate computers sharing images of child pornography. The databases identified a computer using IP address 72.48.82.156 that was making available for download known images/videos of child pornography.

While conducting a search of files available for download, SA Kris Knight found that IP address 72.48.82.156 made available for download three files, containing known images of child pornography previously identified by law enforcement officials. The files were identified by their unique hash identifiers. A hash identifier is the result of a block of data that has been assigned an algorithm generated hash value, or hash identifier, such that any (accidental or intentional) change to the data will change the hash value.

The three files containing child pornography were made available for download between May 23, 2014, and June 2, 2014. Some files were made available on more than one occasion. In total, there were 100 occasions that known child pornography was made available for download from the IP address 72.48.82.156 between May 23, 2014, and June 2, 2014.

Below are the three file names made available to share from IP address 72.48.82.156:

- - xxx anal oral niÃfÃ±a 11 aÃfÃ±os.mpg
- niÃfÃ±a 6 aÃfÃ±os mamando verga-porno infantil-xxx.avi
- porno infantil extremo\_niÃfÃ±itas cojidas.mpg

From my training and experience, I recognize that the last two titles are in Spanish. The file titled "porno infantil extremo\_niÃfÃ±itas cojidas.mpg" roughly translates into English as, "Extreme infant porn...fucking". The file titled "niÃfÃ±a 6 aÃfÃ±os mamando verga-porno infantil-xxx.avi" roughly translates into English as, "Dick sucking-infant porn-xxx".

Grande Communications was presented with a court order for subscriber and billing information to include: subscriber information, billing records, records of session times and durations, time of registration, and log-in IP address for both IP addresses mentioned above.

Nuestar, doing business as (dba) Grande Communications, complied with the court order and delivered the following report:

Target details: IP Address 72.48.82.156  
Customer Name: Al Weinkauff  
Customer Address: 516 N. Loop 250 West, Apt. 1601, Midland, Texas 79703  
Email Address: a2w@grandecom.net

Government database checks show that Albert "Al" Weinkauff (date of birth August 11, 1949) lived at 516 N. Loop 250 West, Apt. 1601, Midland, Texas 79703 until recently. Government database and Texas Department of Motor Vehicles records show that Albert "Al" Weinkauff (date of birth August 11, 1949) currently resides at 6105 Spahn Street, Midland, Texas 79706. Database checks for Al Weinkauff revealed no criminal history.

HSI Midland Special Agents conducted surveillance on the residence located at 6105 Spahn Street, Midland, Texas 79706. The residence is a single story home with brown, tan, and grey brick siding. The home has tan stone and wood trim. The numbers "6105" are affixed to the home on a plaque.

During surveillance, one vehicle was noted at the residence. The vehicle is a white SUV bearing Texas license plate 292 5AY. Records checks show that that license plate was cancelled in 2012.

On January 30, 2015, Special Agent Knight viewed two videos matching the hash identifiers IP address 72.48.82.156 made available for download on the Peer to Peer (P2P) file sharing Ares network.

The first video was titled niÃfÃ±a 6 aÃfÃ±os mamando verga-porno infantil-xxx.avi and was identified using hash identifier 5UDNV6G2MFYSBVJSINYRSG44PVTYTX6W. The video is approximately one minute and six seconds in duration. This video depicts a prepubescent female child naked performing oral sex on an unidentified male. 15 seconds into the video, the video slows down and depicts the male ejaculating into the child's mouth while he holds onto her hair. The child appears to be 7 years old.

The second titled - xxx anal oral niÃfÃ±a 11 aÃfÃ±os.mpg and was identified using hash identifier 7D6JCMRYSUSQ64V477COHPRZJGJHNU2A. The video is approximately twenty-three minutes and thirty seconds long. The video depicts a clothed 8 to 10 year old pre-pubescent girl looking at pornographic magazines. A clothed adult male appears in the room with the young girl and begins to look at the magazines with her. The young girl and the adult male then become completely naked, exposing their genitals for the camera. In the video, the young girl is anally raped by the adult male.

Additionally, the adult male uses his fingers to vaginally penetrate the girl. The girl is also orally raped by the adult male.

### **CHARACTERISTICS COMMON TO COLLECTORS OF CHILD PORNOGRAPHY**

Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have consulted, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

- a. A person who has a sexual interest in children may receive sexual gratification, stimulation, and satisfaction from contact with children or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. A person who has a sexual interest in children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. A person who has a sexual interest in children oftentimes uses these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. A person who has a sexual interest in children almost always possesses and maintains their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. A person who has a sexual interest in children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years. Child erotica is defined as: Materials or items that are sexually arousing to certain individuals but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.
- d. Likewise, a person who has a sexual interest in children often maintains their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the person's residence, to enable the person to view the collection, which is valued highly.



e. A person who has a sexual interest in children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other persons who have a sexual interest in children; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Persons who have a sexual interest in children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Based upon my training and conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography, I am aware that individuals who access paid subscription or free sites offering images and/or videos depicting child pornography do so for the purpose of downloading or saving these images to their hard drive or other storage media so that the images and videos can be added to their collection.

Based upon my training and conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography, I am aware that individuals who share and distribute child pornography are often persons who have a sexual interest in children who have escalated their activity from anonymously obtaining images of child pornography to proactively distributing images they have collected, often for the purposes of trading images of child pornography with others as a method of adding to their own vast collections. From my training and experience, I know that individuals involved in the distribution of child pornography also continue to obtain images of child pornography found elsewhere on the Internet, e.g. Newsgroups and Web sites, and paid subscriptions.

In addition, based upon the conduct of individuals involved in the collection of child pornography as set forth above, namely that they tend to maintain their collections at private locations for long periods of time, there is probable cause to believe that evidence of the offenses of distributing and possessing child pornography is currently located at the ("SUBJECT PREMISES"). Based on past investigations and experience with other similar cases your affiant believes that a collector can preserve his preferred images for years or reacquire them upon conviction and release back into society.

Based upon my training and experience, and conversations with other law enforcement officers, I am aware that often perpetrators of child pornography store and/or transport digital storage devices and other related digital items in vehicle to which they have access.



## **BACKGROUND REGARDING THE SEIZURE OF COMPUTERS**

Based on my knowledge, training, experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

Computer storage devices (like hard drives, diskettes, tapes, laser disks, Bernoulli drivers and others) store the equivalent of thousands of pages of information. Especially when a user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires search authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on-site.

Searching computer systems for criminal evidence is a highly technical process requiring expert skill in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices.

Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of facilitating a criminal violation

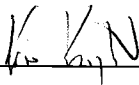
and should all be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

In my training and experience, persons conducting electronic transactions via computers and the Internet, routinely print hard copies of such documents, to memorialize the transaction.

### **CONCLUSION**

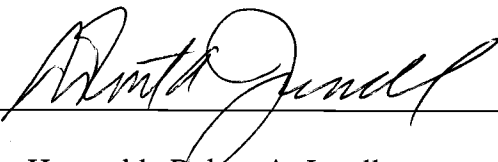
Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the premises described in Attachment A, in violation of 18 U.S.C. Section 2252 and that the violations have occurred and continue to occur at the premises.

I, therefore, respectfully request that attached warrant be issued authorizing the search of 6105 Spahn Street, Midland, Texas 79706 (more fully described in Attachment "A") and the seizure of evidence (more fully described in Attachment "B")

  
\_\_\_\_\_

Kris Knight, Special Agent  
Homeland Security Investigations

Sworn to and subscribed before me this 6<sup>th</sup> day of February, 2015

  
\_\_\_\_\_

The Honorable Robert A. Junell  
United States District Judge

## ATTACHMENT A

### DESCRIPTION OF PREMISES TO BE SEARCHED

The residence, located at 6105 Spahn Street, Midland, Texas 79706, is a single story home with brown, tan, and grey brick siding. The home has tan stone and wood trim. The numbers "6105" are affixed to the home on a plaque.

A white SUV bearing Texas license plate 292 5AY was parked in the driveway of the residence. Records checks show that that license plate Texas 292 5AY was cancelled in 2012.

The search may include: one white SUV bearing Texas license plate 292 5AY.

## ATTACHMENT B

### ITEMS TO BE SEIZED

Items to be seized include any and all evidence, fruits and instrumentalities pertaining to violations of Title 18 United States Code, Section 2252 and which may be more particularly described as follows:

Any instructions, programs or recording stored in the form of electronic or magnetic media which are capable of being intercepted by a computer or related components. The items to be seized include operating systems, application software, utility programs, compilers, interpreters, and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio or other means of transmission.

Electronic devices, computer hardware, software, passwords, data security devices, and computer-related documentation. Electronic devices and computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices, (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct

All cellular phones, laptops, netbooks, e-books, tablets, and any other electronic media storage devices.

This is property that constitutes evidence of the commission of a criminal offense and property designed and intended for use and which is and has been used as the means of committing a criminal offense in violation of Title 18 United States Code, Section 2252.

## UNITED STATES DISTRICT COURT

for the  
Western District of TexasIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)6105 Spahn Street, Midland  
Texas 79706Case No. MO:15-MJ-064

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Western District of Texas  
(identify the person or describe the property to be searched and give its location):

6105 Spahn Street, Midland, Texas 79706 (More fully described in Attachment "A")

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment "B"

**YOU ARE COMMANDED** to execute this warrant on or before 2/20/15 (not to exceed 14 days)  
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to David Counts  
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☐ for        days (not to exceed 30) ☐ until, the facts justifying, the later specific date of       Date and time issued: 2-6-15 10:51 AM  
Judge's signatureCity and state: Midland, TexasRobert A. Junell United States District Judge  
Printed name and title

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory of the property taken and name of any person(s) seized:

## Printed name and title

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The residence, located at 6105 Spahn Street, Midland, Texas 79706, is a single story home with brown, tan, and grey brick siding. The home has tan stone and wood trim. The numbers "6105" are affixed to the home on a plaque.

A white SUV bearing Texas license plate 292 5AY was parked in the driveway of the residence. Records checks show that that license plate Texas 292 5AY was cancelled in 2012.

The search may include: one white SUV bearing Texas license plate 292 5AY.



## ATTACHMENT B

### ITEMS TO BE SEIZED

Items to be seized include any and all evidence, fruits and instrumentalities pertaining to violations of Title 18 United States Code, Section 2252 and which may be more particularly described as follows:

Any instructions, programs or recording stored in the form of electronic or magnetic media which are capable of being intercepted by a computer or related components. The items to be seized include operating systems, application software, utility programs, compilers, interpreters, and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio or other means of transmission.

Electronic devices, computer hardware, software, passwords, data security devices, and computer-related documentation. Electronic devices and computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices, (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct

All cellular phones, laptops, netbooks, e-books, tablets, and any other electronic media storage devices.

This is property that constitutes evidence of the commission of a criminal offense and property designed and intended for use and which is and has been used as the means of committing a criminal offense in violation of Title 18 United States Code, Section 2252.